

UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors: COLLINS et al.

Docket No: 20206-0014(PT-TA-410)

Patent No: 5,848,159

Issued: December 8, 1998

For: "PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"

Assistant Commissioner for Patents  
Box: Reissue  
Washington, D.C. 20231


TRANSMITTAL FOR INFORMATION DISCLOSURE STATEMENT

Enclosed for filing in the above-identified application is an Information Disclosure Statement with attached Form PTO-1449 and copies of cited references.

The Commissioner is authorized to charge any required fees, or credit any overpayment to Deposit Account No. 02-3964 (Order No. 20206-0014(PT-TA-410)).

Dated:

Respectfully submitted,



LEAH SHERRY

Reg. No. 43,918

OPPENHEIMER WOLFF & DONNELLY LLP  
CUSTOMER NO. 25696  
1400 Page Mill Road  
Palo Alto, CA 94304  
Telephone: 650-320-4000  
Facsimile: 650-320-4100

# 1514

JCS14 U.S. PTO  
09/694416  
10720700

UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: **Collins et al.**  
U.S. Patent No: **5,848,159**  
Issue Date: December 8, 1998

Docket No: 20206.14 (PT-TA-410)

For: **"PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"**

Assistant Commissioner for Patents  
Box: Reissue  
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT

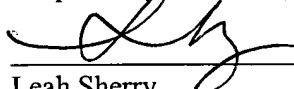
Applicants submits herewith the references listed on the attached form PTO-1449 of which Applicants are aware which are believed to be material to the examination of this application and in respect of which there may be a duty to disclose in accordance with 37 CFR 1.56.

The filing of this information disclosure statement shall not be construed as a representation that a search has been made (37 CFR 1.97(g)), nor as an admission that the information cited is, or is considered to be, material to patent ability, nor an admission that no other material information exists.

Respecting for example reference AC, the paper entitled "Using Four-Prime RSA in Which Some of the Bits are specified," Applicants believe that this reference teaches away from the claimed invention. For instance, reference AC does not cover instances where the number of primes is  $K=3$  and  $K>4$ . Reference AC merely teaches the extension of 2 prime factors to 4 prime factors for a greater modulus  $n$ . What is more, the 4 prime factors of  $n$  are not random but, rather, related through a relationship of the form  $p_i = 2^k f_i + a_k$ . Namely, reference AC teaches a method for determining 4 related primes such that the number of bits required to represent the primes is less than the sum of their length. (See: S.A. Vanstone et al. p. 2118).

The filing of this information disclosure statement shall not be construed as an admission against interest in any manner. Notice of January 9, 1992, 1135 O.G. 13-25, at 25.

Respectfully submitted,

  
\_\_\_\_\_  
Leah Sherry  
Reg. No: 43,918

DATE: September 27, 2000

OPPENHEIMER WOLFF & DONNELLY LLP  
1400 Page Mill Road  
Palo Alto, CA 94304  
Tel: (650) 320-4000  
Fax: (650) 320-4100